29.   In a rights management data processing architecture including an

electronic appliance that interacts with an application through an interface, a method of

interoperating with a secure electronic container comprising the following steps:

at the electronic appliance, providing a descriptive data structure to the

application, the descriptive data structure including information regarding a security

feature of an electronic appliance or of software running on an electronic appliance;

(b) at the electronic appliance, checking to determine whether the electronic

appliance or software running on the electronic appliance contains the security feature;

(c) if the electronic appliance or software contains the security feature, the

application generating a request for a secure container, the request being based at least

in part on the descriptive data structure;

(d) receiving the secure container at the electronic appliance; and

(e) using the electronic appliance to access the secure container.

30.   A method as in Claim 29 further including the steps of:

(f) at the electronic appliance, providing information from the secure container to

the application; and

(g) processing the provided information at least in part based on information

contained in the descriptive data structure.

31.   A method as in Claim 30 wherein the processing step (g) includes processing the provided information in accordance with metadata contained in the descriptive data structure.

32.   A method comprising:

(a) creating a descriptive data structure that defines a first and a second type of secure container structure, the first type and the second type differing at least in a security specification;

(b) using the descriptive data structure to create a first secure container of the first type and a second secure container of the second type;

(c) distributing a copy of the descriptive data structure to an electronic appliance;

(d) checking a security aspect of the electronic appliance or of software running on the electronic appliance;

(e) comparing the checked security aspect to the security specification information in the descriptive data structure;

(f) distributing the first secure container to the electronic appliance if the security aspect of the electronic appliance or software running on the electronic appliance matches the security specification for the first type of secure container, or distributing the second secure container to the electronic appliance if the security aspect of the electronic appliance or software running on the electronic appliance matches the security specification for the second type of secure container; and

(g) interoperating with the distributed secure container at the electronic appliance by using the descriptive data structure to locate or specify information within the distributed secure container.

33.   A method as in Claim 32 wherein the descriptive data structure corresponds to an atomic transaction, and the method further includes the step of performing the atomic transaction at the electronic appliance at least in part in accordance with the descriptive data structure.

34.   A method as in Claim 32 further including storing the descriptive data structure in a third secure container prior to the distributing step (c), the third secure container including or having associated a rule governing use of at least a portion of the descriptive data structure; and

the comparing step (e) occurs at least in part under the control of the rule.

35.   A method as in Claim 32 further including the step of defining a descriptive data structure class based on a parameter.

36.   A method of achieving a degree of compatibility with a secure environment comprising:

creating a descriptive data structure;

associating the descriptive data structure with an object;

presenting the object and associated descriptive data structure to the secure environment; and

selectively interoperating with the presented object based on the degree to which the secure environment can trust the source of the object or the descriptive data structure.

37.   A descriptive data structure relating to a secure container, the descriptive data structure including the following:

a description of the organization of data contained in the secure container;

a description of a security-related aspect of an electronic appliance or of software running on an electronic appliance;

a first rule requiring that the secure container can only be accessed in an electronic appliance having the security-related aspect or containing software with the security-related aspect; and

a specification requiring that the secure container be at least in part governed by the first rule.

38.   A descriptive data structure as in Claim 37, in which:

the data organization description specifies that the data is organized into a first section and a second section.

39.   A descriptive data structure as in Claim 38, further including:

a second rule at least in part governing use of data in the first section and a third rule at least in part governing use of data in the second section; and

a specification requiring that the secure container be at least in part governed by the second rule and the third rule.

40.   A method including:

generating a descriptive data structure in a first environment characterized by a first security aspect;

specifying information in the descriptive data structure including information relating to the first security aspect, a first rule, and a second rule;

transmitting the descriptive data structure to a second environment;

at the second environment, retrieving the information relating to the first security aspect from the descriptive data structure; and

determining whether to use the first rule or the second rule based on the first security aspect information.

41.   The method of Claim 40, wherein the determining step includes using the first security aspect information to determine the level of security present at the first environment.

42.   The method of Claim 40, wherein the determining step includes determining to use the first rule or the second rule, but not both.

43.   The method of Claim 40, wherein specifying information in the descriptive data structure includes populating a first target block and a second target block.

44.   A descriptive data structure embodied on a computer-readable medium or other logic device, including the following elements:

identification information at least in part identifying a first rights management data structure;

organization information at least in part describing the organization of at least some governed information contained within or referenced by the first rights management data structure; and

rule information relating to a first rule used to at least in part govern use of at least a portion of the governed information contained within the first rights management data structure, the first rule identifying an element of an environment, the element being required for at least one use of the governed information.

45.   The descriptive data structure of Claim 44 in which the first rights management data structure is a secure container.

46. The descriptive data structure of Claim 45, in which the secure container includes:

the governed information; and

the first rule.

47. The descriptive data structure of Claim 45, in which the secure container includes the descriptive data structure.

48. The descriptive data structure of Claim 44, in which:

the first rule is stored outside the descriptive data structure; and

the rule information includes information regarding the location at which the first rule is stored.

49. The descriptive data structure of Claim 44, in which:

the rule information also relates to a second rule, the second rule being a display rule at least in part governing the display of at least a portion of the governed information.

50.   The descriptive data structure of Claim 44, in which:

the governed information includes source information at least in part identifying an author, creator, publisher or owner of at least a portion of the governed information; and

the rule information also relates to a second rule, the second rule requiring display of the source information under at least some circumstances.

51.   The descriptive data structure of Claim 44, in which:

the rule information also relates to a second rule, the second rule constituting a creation rule at least in part governing the creation of a specific example of the first rights management data structure.

52.   The descriptive data structure of Claim 51, in which:

the second rule at least in part specifies information that must be included with the specific example of the first rights management data structure.

53.   The descriptive data structure of Claim 44, in which:

the descriptive data structure is stored in a second rights management data structure.

54.   The descriptive data structure of Claim 44, further including:

information relating to the organization of at least some information contained in a second rights management data structure that differs in at least one respect from the first rights management data structure.

55.   The descriptive data structure of Claim 44, in which:

the organization information includes information relating to the location of at least some of the governed information.

56.   The descriptive data structure of Claim 44, further including:

a first target data block including information relating to a first target environment in which the descriptive data structure may be used.

57.   The descriptive data structure of Claim 56, further including:

a second target data block including information relating to a second target environment in which the descriptive data structure may be used.

58.   The descriptive data structure of Claim 44, further including:

a source message field containing information at least in part identifying at least one source for the descriptive data structure.

59.   The descriptive data structure of Claim 58, in which:

the source identification information includes source environment information relating to at least one aspect of an environment in which the descriptive data structure was at least in part created.

60.   The descriptive data structure of Claim 59, in which:

the source environment information includes information relating to security present at the environment in which the descriptive data structure was at least in part created.

61.   The descriptive data structure of Claim 44 further including a source seal.

62.   The descriptive data structure of Claim 61, in which:

the source seal includes a hash of at least a portion of the descriptive data structure.

63.   The descriptive data structure of Claim 61, in which:

the source seal is encrypted based on a private key.

64.   The descriptive data structure of Claim 63, further including:

key location information related to a location from which a public key corresponding to the private key may be obtained.

65.   The descriptive data structure of Claim 64, in which:

the key location information is contained within a certificate.

66.   The descriptive data structure of Claim 65, in which:

the certificate is contained in the descriptive data structure.

67.   A distributed data processing arrangement including:

a first data processing apparatus including:

a central processing unit, and

a first memory storing a descriptive data structure, the descriptive data structure including information regarding a first organization of elements within a secure container; and

a second data processing apparatus including:

a central processing unit, and

a second memory storing a first secure container including:

data elements organized at least in part in accordance with the information contained in the descriptive data structure, and

a rule set used to at least in part govern an aspect of access to or use of the data elements, the rule set including:

a first rule requiring that information regarding a use of one of the data elements be at least temporarily recorded, and

a second rule requiring that use of one of the data elements only occur in a data processing apparatus including a specified element.

68.   The distributed data processing arrangement of Claim 67, in which:

the descriptive data structure is contained in a second secure container that also includes a rule at least in part governing use of at least a portion of the descriptive data structure.

69.   The distributed data processing arrangement of Claim 68, further including metadata relating to the contents of the second secure container.

70.   The distributed data processing arrangement of Claim 69, in which the metadata is stored in the second secure container.

71.   The distributed data processing arrangement of Claim 69, in which:

the metadata is stored in a third secure container.

72.   The distributed data processing arrangement of Claim 71, further
including:

a third data processing apparatus including:

a central processing unit;

a third memory including the third secure container and a rule used to at
least in part govern at least one aspect of access to or use of the metadata; and

communications means by which the third data processing apparatus may

communicate the third secure container, or a copy of the third secure container,

to the second data processing apparatus.

73.   The distributed data processing arrangement of Claim 67, further
including:

a computer program designed to use at least a portion of the descriptive
data structure in an operation on the first secure container or the contents of the first
secure container.

74.   The distributed data processing arrangement of Claim 73, in which the
computer program is designed to use the information regarding the organization of

-14-

elements within the first secure container to identify or locate at least one of the elements.

75. The distributed data processing arrangement of Claim 73 in which:

the computer program includes a browser that uses the information regarding the organization of elements within the first secure container to control, at least in part, the display of at least some information from the first secure container.

76. The distributed data processing arrangement of Claim 73, in which:

the computer program is integrated into an operating system.

77. The distributed data processing arrangement of Claim 76, in which:

the operating system is compatible with at least one version of Microsoft Windows.

78. The distributed data processing arrangement of Claim 73, in which:

the computer program includes means for using a rule from the rule set to govern at least one aspect of the computer program's use of at least a portion of the first secure container contents.

79.   The distributed data processing arrangement of Claim 67, in which:

the rule set includes a third rule at least in part controlling at least one aspect of an auditing process.

80.   The distributed data processing arrangement of Claim 67, in which:

the rule set includes a third rule at least in part controlling at least one aspect of a budgeting process.

81.   The distributed data processing arrangement of Claim 67, in which the second data processing apparatus includes a secure electronic appliance.

82.   A method of creating a first secure container, including:

(a) accessing a descriptive data structure, which includes or contains location information regarding:

organization information at least in part describing a required or desired organization of a content section of the first secure container, and

metadata information at least in part specifying a step required or desired in creation of the first secure container;

(b) organizing information contained in the first secure container using the descriptive data structure; and

-16-

(c) using the metadata information to at least in part generate or identify a first control designed to govern at least one aspect of access to or use of at least a portion of the information contained in the first secure container, the first control specifying that the access or use may only occur at a device which contains a specified attribute.

83.   The method of Claim 82, in which the descriptive data structure is contained in a second secure container and accessing the descriptive data structure includes:

complying with a second control associated with the second secure container.

84.   The method of Claim 82, further including:

(d) using the metadata information to at least in part identify or generate a second control to govern an aspect of access to or use of at least a portion of the information contained in the first secure container.

85.   The method of Claim 84, further including:

(e) associating the second control with the first secure container.

86.   The method of Claim 82, further including:

(f) receiving the descriptive data structure at a first site from a second site prior to accessing the descriptive data structure; and

(g) creating the first secure container at the first site.

87.   The method of Claim 86, in which:

the descriptive data structure is received at the first site in a second secure container which is governed at least in part by a second control; and

accessing the descriptive data structure is governed at least in part by the second control.

88.   The method of Claim 86, in which:

the metadata is not contained within the descriptive data structure, but the descriptive data structure includes information regarding the location of the metadata, and further including:

(h) receiving the metadata at the first site prior to using the metadata, the metadata being received separately from the descriptive data structure.

89.   The method of Claim 88, further including:

(i) requesting the metadata by the first site based on information contained in the descriptive data structure.

90.   The method of Claim 88, wherein receiving the metadata includes:

receiving the metadata at the first site in a second secure container having associated a second control; and

wherein using the metadata in the generation or identification of the first control occurs after the first site has complied with a requirement imposed by the second control.

91.   The method of Claim 82, further including:

(d) storing owner or creator information in the first secure container in compliance with the descriptive data structure.

92.   The method of Claim 91, further including:

(e) storing copyright ownership information in the first secure container in compliance with the descriptive data structure.

93.   The method of Claim 92, further including:

(f) storing an advertisement in the first secure container in compliance with the descriptive data structure.